Arab Republic of Egypt

Ministry of Communications and Information Technology

www.mcit.gov.eg

e-Government Network and Messaging Standard

Table of Content

Document Revision History

Date	Version	Updated By	Description of Changes
3/6/2002	1.0	Network and messaging Workgroup	First Draft (Index of the Content)
6/2/2002	1.1	Network and messaging Workgroup	Details of the Index
10/07/02	1.2	General Dynamics	Complete Editing and Re-organization

1 Introduction

The e-Government networking and messaging workgroup mission is to set out the Egyptian Government's framework requirements to provide Networking Services and to implement a standard messaging and collaboration system for the Government of Egypt's entities. In this document, some of the industry standards of the networking and messaging services will be described. The basic recommended guidelines that need to be met in any government networking and messaging implementation will be extracted from these industry standards. The document focuses only on two sections, the first one is about Network Operating System Services and the second one is related to Messaging and Collaboration Services.

We will start by Section-2 to describe quickly the proposed E-Government architecture. Section-3 will explain the Networking File Services and Section-4 will do the same for the Networking Print Services. The messaging services will be briefly discussed in Section-5.'

2 E-Government Architecture

Conceptually, architecture is a design of components and their defined interfaces in a system. Domains are simply topics of architecture. IT architecture has a certain typical domains such as application, data and infrastructure. A high-level conceptual e-government architecture is depicted in Figure-1. It consists of the following layers:

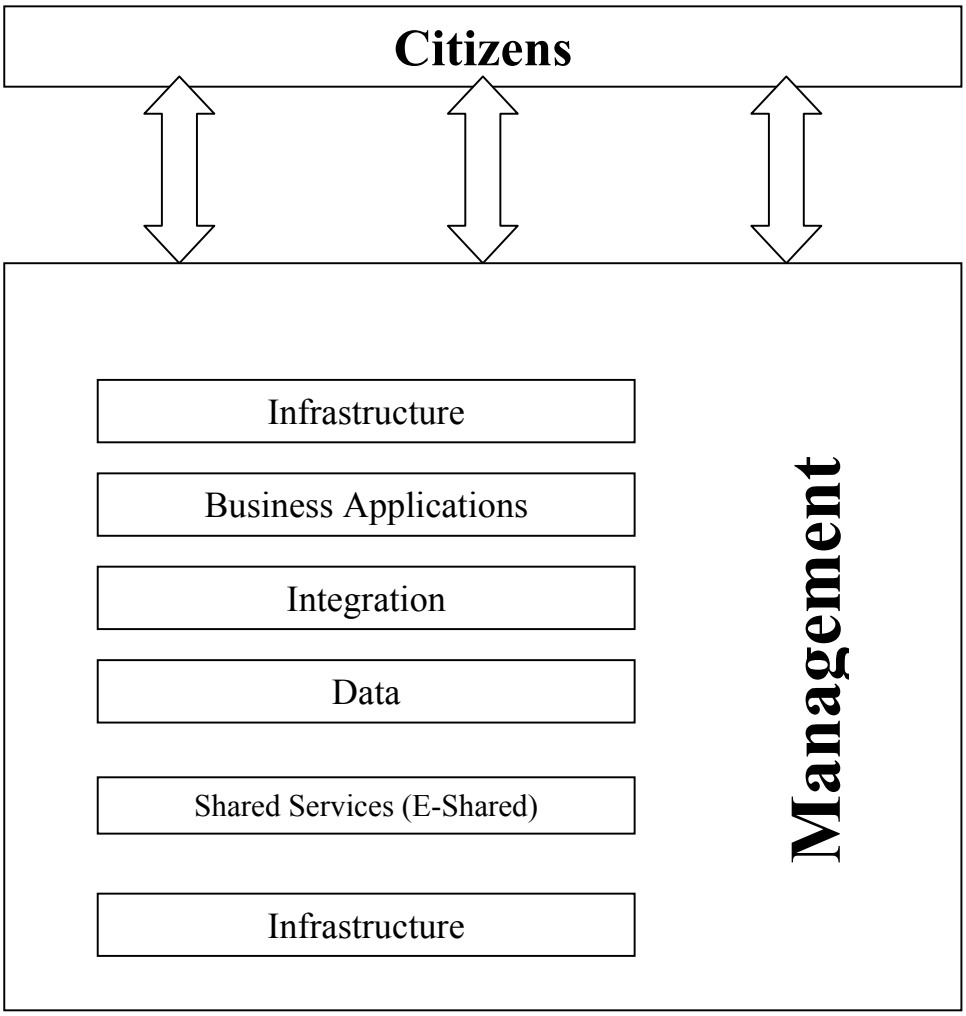

Figure 1: A high level Conceptual E-Government architecture.

Customer Interface Layer: The e-government architecture provides for multiple channels into government and supports G2C, G2B, G2E and G2G interactions. This layer also abstracts business logic from the interface to allow different devices to have access to the same business rules. A key function of this layer is the ability to match a customer to the customer record to ensure a unified customer history. This also ensures the multi-channel customer centricity that is required to effectively serve the customer.

Business Application Layer: This layer includes e-business applications and bulk transfers of information to and from government's business partners and other governments. It also includes legacy applications.

Integration Layer: This layer includes middleware that facilitates consistent requests and responses among business applications and shared services, while insulating these applications and services and data from direct manipulation. Middleware also supports heterogeneous operating environments.

Shared Services (e.g., E-Shared) Layer: This layer includes a set of common services that are independent from particular business applications, but they support these applications. Shared services, of necessity, need to be managed centrally, perhaps by the central IS organization or its service partners. Any service that can support multiple business applications and is devoid of agency- or industry-specific business logic is a candidate for a shared service. Payment services, for example, can be generically used by multiple business applications or Community of Interest (COI) applications, such as environmental permits, vehicle registrations and surplus auctions. Examples of shared services for e-government include **networking services**, directory services, **messaging** (e.g., e-mail), identification, and authentication infrastructures. Shared services are a key component of the e-government architecture. They make it possible to present and execute a well-organized, enterprise-wide service delivery. Without shared services, there is no foundation for effective service delivery, and wasted effort and money in building duplicate services. This paper will focus on the networking and messaging services of the E-shared layer. The file and print services will the main points to be explained under the networking services.

Data Layer: This includes COI, legacy and decision support databases. A consistent image of customer identity is paramount in the new architecture. While customer participation in specific government programs may be shielded from the public due to legal privacy mandates, identity should be maintained separately and consistently to allow reuse among systems. Metadata should be created and marketed for common data elements to ensure consistent usage.

Infrastructure Layer: Includes platforms, user devices and networks. The emphasis here is on reliability and availability. In addition to using redundant components, this layer is supported heavily by the systems management layer.

Management Layer: All of the above layers provide a basic structure for e-government. They require, however, a management structure and set of processes that support and sustain them. The management layer consists of a concentric set of progressively more-encompassing sub-layers that achieve this function. Building from the inside out, each sub-layer operates within the context of the next higher sub-layer. The sub-layers, in order, are:

- Security
- Systems Management
- Standards
- Architecture Management
- Policies
- Governance
- Marketing and Training

3 File Services

The majority of network operating systems (NOS) provide file services; that is, they offer centralized file storage that lets users easily share files. File servers often store private files as well as shared files, and provide a single point of backup for both. File servers let users access their files even when they move to different workstations. The Network Operating System should introduce management of network shares and users and to the file system. In addition, NOS support several other on-disk file system types. The file system protocol is the communication vehicle to move files from one location to another.

In the next sub-sections, some of the NOS file-system related features will be explained.

3.1 Managing Shares, Connected Users, and Open Files

Centralized management framework for hosting administrative tools, which provides commands and tools for authoring consoles. The Shared Folders management tool should be a file–system-related tool in the server operating system. The tool should enable the creation of shares, manages the connections on local or remote computers, and displays open files. The file share management tool should be able to publish the shared folder as a Volume Object in the directory service to enable users to query available resources and shares.

Administrators should be able to perform the following tasks:

- **Shares.** Create, view, and set permissions for network shares, including shares running on previous version of the operating system.
- **Sessions.** View (and disconnect) users connected to the computer over the network.
- **Files.** View (and close) files opened by remote users.

3.2 Data and File Access

The data access feature should provide intelligently designed data access features to accommodate remote users. These features provide transparent synchronization of files and directories with the corporate network. They should increase efficiency and reduce the amount of error, needless resource consumption, security compromise, and loss of data that arises from uncontrolled replication of important data and document to floppy disks, multiple hard drives, and e-mail attachments.

3.3 File System Types

3.3.1 UNIX File System (UFS)

3.3.2 Veritas File System (VxFS)

3.3.3 Microsoft NT File System (NTFS)

Microsoft has introduced the NTFS, a 64-bit advanced file system for storing data on hard disk. The NTFS supports the following features:

- **File-level access control:** The NTFS governs which users and groups can access individual files and directories, and it can provide varying levels of access for different users. This is then enforced by the core operating system. The File System should have file permissions like No Access, List, Read, Add, Add and Read, Change, Full Control, Special Directory Access, and Special File Access (which provides an even greater degree of granularity). File-level access control does not include file encryption.
- **Compression:** The NTFS compression allows for the compressed storage of files and directories so that less physical space is required. Compression is configurable on a volume, directory, or file basis. With File System, if anything goes wrong physically with a portion of data in a compressed file, only that file is affected.
- **Recovery log:** The NTFS logs all changes to the file system so that every file or directory update can be redone or undone to correct discrepancies caused by system failure or power loss. The NTFS cluster remapping—called sector/cluster hot fixing—repairs hard disk failures on the fly without returning error messages to the calling application. If the data is corrupt, NTFS flags that part of the hard disk as defective, and then rewrites the data to another location. Recovery log operations are fast and transparent to users.
- **POSIX support:** The NTFS file names support the Portable Operating System Interface standard for network naming conventions, such as case sensitivity, last-access time stamping, and hard links.

Some of the NTFS enhancements are:

- File System reparse points and file system filter drivers
- Encrypting File System (EFS)
- File System volume mount points
- File System sparse file support
- Native property sets
- Security ID (SID) searching and bulk access control list (ACL) checking
- File System Change Journal
- Distributed Link Tracking

3.3.4 Novell iFolder File System

The Novell iFolder server software was presented on NetWare 6 to provide several features to the users. The iFolder consists of a server and client component where it can be accessed via a web-based browser for file upload and download. At the same time, it does not require any client software. Configuration details between the client and server to handle synchronization functions are easily set and easy to change. Both the client and the server sides include simple management and control utilities. Some of the Novell iFolder features are:

- Encryption Options
- Automatic Compression
- Browser and PDA access
- Bandwidth efficiency
- LDAP (Lightweight Directory Access Protocol) Authentication
- Synching from Server to Client
- Easy Administration
- Policy Options

3.3.5 Distributed File System (DFS)

DFS presents to users a logical view of distributed physical storage, making both managing and finding network data easier. It is not a new file system but software that gives users a view of what *looks like* a unified hierarchical file system, even though the data is in reality distributed in different locations. For example, you can use DFS to make marketing files scattered across multiple servers in a domain appear as if all these files reside on a single server. This eliminates the need for users to go to multiple locations on the network to find the information they need. DFS can connect hundreds or thousands of published shares in a single logical system.

Users use the DFS Administrator tool to administer DFS volumes. Implementing DFS is not mandatory, but network administrators should consider doing so if:

- The users accessing shared resources are distributed across multiple sites.
- Most users require access to multiple file servers.
- Network load balancing can be improved by redistributing shared resources.

- Users require uninterrupted access to file servers.
- The organization uses either internal or external Web sites.

DFS should be protocol independent, which means that any platform can be included in the DFS namespace. The DFS client and server use the Common Internet File System (CIFS) to determine which file server will be accessed by the client. When the client then accesses the target file server, it uses the native protocol to access the file server.

The purpose of DFS is to let users and applications access files. DFS is *not* designed to perform operations such as indexing, virus scanning, or backup, because accessing very large numbers of files in a highly sequential/repetitive manner using DFS would substantially increase network traffic. In addition, when using DFS replicas you do not know which particular file server in a replica set is being accessed, which means that DFS is not suitable for backup and restore operations.

3.3.6 Other File Systems

Network Operating Systems (NOS) should support multiple file systems. Some provide backward compatibility and others offer access to the latest storage media.

- **FAT16.** Format the partition using FAT16 if the installation partition is smaller than 2 GB, or if you are dual booting Windows 2000 and MS-DOS or Windows 3.1.
- **FAT32.** Format the partition using FAT32 if the installation is 2 GB or larger and you are dual booting with Windows 95 OSR2 or Windows 98.
- **Compact Disk (CD) File System**

The Server Operating system should support the Compact Disk File System (CDFS), which lets data be read from CD-ROM devices. For CDFS specs please see ISO[1] 9660 specification.

- **Universal Disk Format (UDF)**

The Server Operating system should support for the Universal Disk Format (UDF) file system defined by the Optical Storage Technology Association (OSTA)[2]. UDF is compliant with ISO-13346; The server operating system should support version 1.5. UDF is the successor to CDFS (ISO 9660), and is also used for data interchange between operating systems and for digital versatile disk (DVD).

3.4 File Access Protocols

File access protocols remain a mixture of standards (FTP and HTTP) and proprietary formats (CIFS, AFP, and NFS). File Transfer Protocol (FTP) came from IETF (Internet Engineering Task Force) early on in the days of TCP/IP standardization. HTTP (Hyper Text Transfer Protocol), developed by Tim Berners-Lee for the World Wide Web (WWW), comes under the standards jurisdiction of the W3C (World Wide Web Consortium).

[1] ISO, though not an acronym, stands for the International Organization for Standardization, an international organization that defines standards for designing networks.
[2] OSTA is an international trade association that promotes the use of writeable optical technology for storing computer data and images.

The other file protocol "standards" earned their reputation as a standard by market penetration rather than committee vote.

3.4.1 Common Internet File System (CIFS) Protocol

CIFS comes from Microsoft, building upon SMB (Server Message Block) protocol used in NETBIOS file sharing. Called a "public" variation of SMB, CIFS has been proposed to the IETF to become an Internet Application Standard, but Microsoft developed CIFS from the beginning.

3.4.2 Appletalk File Protocol (AFP)

Apple developed AFP, and other vendors who wants to access AFP-based storage must follow Apple's rules.

3.4.3 Network File System (NFS) Protocol

NFS can be called a true distributed file system, and came from "the network is the computer" people at Sun Microsystems. Technically a client-server application, NFS allows remote client to "mount" a local file system at designated mount points. To the remote client, the mounted file system looks exactly like a subdirectory branch structure of the local file system.

3.5 Indexing Service

Network Operating System should include Indexing Service as part of the base features. This development extends the indexing and searching services to locate information on file servers as well as on Web sites.

NOS Indexing Service should be able to index file system objects and Intranet and Internet Web sites across volumes and machines so that they can be searched by network, intranet, and Internet users alike. Making these search activities look similar to the user saves an organization time and money in training and supporting employees. All Indexing Service operations should be automatic, including index creation, index updating, and crash recovery in the event of a power failure.

These Indexing Service features that could be under further investigations are:

- Indexing Service structure
- Catalogs
- Both data and property search
- Search and retrieval
- Indexing control and speed
- Detecting changes using File System Change Journal
- Index storage using sparse streams
- Integrating searches into applications
- Remote storage and retrieval integration
- Mount/dismount tracking

3.6 Storage Management Services

The quantity of data stored on distributed systems has increased exponentially over the last decade. As the number of client/server systems increases in an organization, so does the number of storage subsystems. Up to 25 percent of a typical computing budget is spent on storage. The kind of data stored on client/server systems is changing as well—growth in Internet/intranet usage and in 32-bit/64-bit architectures are major contributors to the changes in types of data found in the distributed network. These developments are accelerating the creation of large volumes of data and resulting in increased storage requirements at proportionately increased cost.

The NOS should offer several features that improve storage and reduce its cost. These include:

- Remote Storage service
- Removable Storage service
- Disk quotas
- The Single Instance Store (SIS)
- System File Protection
- Code Signing and Catalog Files
- Storage support for hardware innovations

3.6.1 Remote Storage

The Remote Storage service, should support Hierarchical Storage Management (HSM), helps manage the cost associated with large quantities of data that must be kept accessible. The Remote Storage hierarchy consists of two layers:

- **Local storage** refers to the file system volumes local to the file server hosting the Remote Storage software.
- **Remote storage** refers to data moved from the local hard disk to a remote storage device (such as tape) that can be recalled whenever needed.

If a file has not been used in the past thirty days, there is a high probability that it will not be accessed again. These infrequently used files consume the majority of disk space, and it is these files that Remote Storage typically migrates to secondary storage. Remote Storage automatically moves data back and forth between high-cost, faster disk drives and low-cost, high-capacity storage media (tape library). Remote Storage monitors the amount of space available on local volumes, and when the amount of free space dips below the needed level, eligible files are transferred from the hard disk to secondary storage. Yet, the user still sees and can still access these archived files. This frees up storage on the file server without requiring the purchase and installation of additional hard disks.

Remote Storage media are not a substitute for primary backup media. Remote Storage is typically used to migrate infrequently used data, so frequently used data, which is more likely to be urgently needed, is less likely to be stored on Remote Storage media. The purpose of Remote Storage is to ensure free space on file server volumes, not to protect enterprise data.

3.6.2 Removable Storage

The Network Operating System should support Removable Storage service manages removable storage media (tapes and optical disks) and robotic storage libraries attached to a computer. Removable Storage moves media around within and between libraries and controls access to that media.

3.6.3 Disk Quotas

Disk quotas; provide enhanced control of network-based storage in a distributed environment. Disk quotas give administrators a powerful tool for managing storage growth.

Members of the Administrators Group can see a Quota tab on the Properties dialog box of an file system-formatted volume. You can use this tab to set disk quotas to monitor and limit disk space use on file system volumes on a per-user basis. You can set disk quotas on both local and remote volumes. Quotas are tracked independently for different volumes, even if the volumes are different partitions on the same physical drive. However, if you have shares on the *same* volume, the quotas assigned to that volume apply to all of these shares collectively, and users' utilization of the shares cannot exceed the assigned quota on that volume.

Disk quotas apply only to volumes and are independent of folder structures. That is, if a user moves a file from one folder to another on the same volume, volume space usage does not change. But if the user copies the file to a different folder on the same volume, the volume space usage doubles.

Within the file system, volume usage data is stored by user security ID (SID), not by user account name. Administrators can set two values: a *warning threshold* and a *hard quota*.

Using the *warning threshold* is useful when tracking disk space use on a per-user basis is the goal rather than limiting disk space usage. In this case, once the warning level is reached, you can have the system generate a system log file entry without sending an error message.

Once the *hard quota* limit is reached, the user cannot move or copy any more data onto the storage device, just as if the user had really run out of disk space. You can configure the system to log an event and return an "insufficient disk space" error when the user has hit his or her quota limit. When this happens, the user cannot write additional data to the volume without first deleting or moving files.

When you enable disk quotas, you can set both the disk quota limit and the disk quota warning level.

When you enable disk quotas for a volume, volume usage is automatically tracked for new users (a new user receives the default quota unless you establish a quota specifically for that user), but existing volume users have no disk quotas applied to them. You apply disk quotas to existing users by adding new quota entries in the Quota Entries window on a file system volume.

Besides being able to implement the quota on an individual user basis, you can use group policy to set the disk quota globally.

The disk quota feature includes other storage features—such as Remote Storage and sparse files—in its calculations. File compression does not affect quota statistics.

3.6.4 The Single Instance Store

The Single Instance Store (SIS), an operating system base component The Server operating system, helps manage disk space by eliminating duplicate files on a volume. SIS replaces duplicate files with links to a

single common store file that contains the actual file data.

SIS consists of a base tracking service, a kernel-mode file system filter driver, reparse points, and sparse files. SIS replaces the duplicate file(s) with a sparse file and an SIS-specific reparse point. The file containing the actual data is renamed with a 128-bit globally unique identifier (GUID) when it is migrated to the common store.

3.6.5 System File Protection

The Server operating system, System File Protection (SFP), is a system service that protects special operating system files. If one of these files is deleted or over-written, SFP replaces the file with the original from a cache that it maintains.

SFP protects system files by detecting when a file replacement is attempted on a protected system file. SFP is triggered when it receives a directory change notification on a file in a protected directory. After this notification is received, SFP determines which file was changed. If the file is protected, SFP looks up the file signature in a catalog (.cat) file to determine if the new file is the correct version. If it is not the correct version, then SFP replaces the newly installed file with either a copy of the protected version or with a copy from the distribution media.

3.6.6 Code Signing and Catalog Files

Code Signing uses the existing Digital Signature cryptographic technology. A hash of the driver binary and relevant information are stored in a *catalog file*, and the .cat file is signed with a Microsoft digital signature. SFP uses the file signatures and catalog files generated by Code Signing to verify whether a protected system file is the correct version. Code Signing is the means of tracking a file's version and creator. SFP is the enforcement mechanism that uses Code Signing signatures and .cat files to keep system files at their correct versions.

3.6.7 Storage Support for Hardware Innovations

Server Operating System should support new storage hardware innovations, including the following three:

- **I_20** relieves the host of interrupt-intensive I/O tasks, greatly improving I/O performance in high bandwidth applications, such as networked video, groupware, and client/server processing. I_20 features include base support, specialized board support for storage cards, and redundant array of inexpensive disk (RAID) cards.

- **Fibre Channel**, a 1-gigabit per second data transfer technology, maps common transport protocols such as Small Computer System Interface (SCSI) and Internet Protocol (IP), merging networking and high-speed I/O into a single connectivity technology. An open standard defined by American National Standards Institute (ANSI)[3] and Open System Interconnection (OSI)[4], Fibre Channel operates over copper and fiber-optic cabling at distances of up to 10 km.
- **IEEE 1394** is a standard for high-speed peripheral interconnect, which combines simple connectivity with bandwidth for multimedia. IEEE 1394 provides a single connection for audio/visual (A/V) data and control.

4 Printing Services

Print services should be a basic feature of the NOS so it can manage printers. This can be hosted on a dedicated print server, or it can be a specialized print server unit. A printer can be connected to a server, a client computer, or directly to the network. However the printer is connected, it is software on the print server that makes the physical printer visible to the network and that accepts print jobs from client computers.

As with file servers, administrators typically install print servers as member servers rather than domain controllers to avoid the administrative overhead associated with the logon and security roles performed by a domain controller. Often, one server acts as both file and print server.

Organizations can share printing resources across their entire network. Clients on a variety of platforms can send print jobs to printers attached locally to the server, across the Internet/intranet, or to printers connected to the network using internal network interface cards, external network adapters, or another server.

4.1 Print Services Protocols:

2.1.1 Novell iPrint (NiP):

NiP solution is based on Internet Print Protocol (IPP) and includes several features including the followings:

- Directory Service (e.g., eDirectory) Integration
- Distributed Print Services such as management and user support.
- Eliminate geographic and network platform constraints.
- HTTP Authentication and SSL are provided for the data sent over the Internet.

2.1.2 Microsoft Internet Printing Protocol (MIPP):

This is also based on Internet Print Protocol (IPP) standard, and therefore its core capabilities are the same as NiP.

[3] Founded in 1918, ANSI is a voluntary organization composed of over 1,300 members (including all the large computer companies) that creates standards for the computer industry.
[4] OSI is an ISO standard for worldwide communications that defines a networking framework for implementing protocols in seven layers.

4.2 Print Services Features:

Printing services should include the following features:

- **Printer pools.** One *logical printer* (printing software component on the print server, represented by the print icon) is set up to send a print job to the first available member of this group of identical physical printers.
- **Printer priority.** When several *logical printers* are set up to send print jobs to one physical printer, an administrator can establish which print jobs take precedence.
- Wide range of printer supported
- Easier installation of local printers (Plug and Play)
- More types of clients
- Advanced printing features
- Simplified print configuration and user interface
- Standard TCP/IP port monitor
- Remote port administration
- Easy-to-find network printers using Directory Services
- Print queue monitoring
- User permissions and group policies
- User settings
- Print server clustering
- Color output quality
- Internet printing

Some of these improvements are described in the following sections:

4.1.1 Easier Installation of Local Printers (Plug & Play)

The automatic configuration of a computer to work with various peripheral devices—includes a simpler setup process for printers. A user installing a printer does not need to know about drivers, printer languages, or ports. Most printers in the market today are Plug and Play and can be detected by Plug and Play technology. The server operating system should support the following printer's standard:

- **Universal Serial Bus (USB) and IEE 1394 printers.** Printers using the latest connector technology, including printers with a USB port or an IEEE 1394 Serial Block Protocol (SBP) 2 port, are detected instantly. When the user inserts the jack into the port, operating system should immediately detects the USB port or IEEE 1394 connection and starts the installation process. By design, USB and IEEE 1394 support *hot swapping* (also called *hot plugging*), which is the ability to add devices to or remove them from a computer while the computer is running and have the operating system recognize the change.
- **Parallel (LPT port) printers.** Printers that connect through a parallel (LPT) port are not immediately detected when the physical connection is made.
- **Infrared-enabled (IR port) printers.** Infrared-enabled printers are also Plug and Play installed, assuming the printer and computer are within one meter of the infrared transceiver in the computer.
- **Non-Plug and Play printers.** Printers connected through a serial port (COM port) and printers

connected directly to the network with a Network Interface Card are not Plug-and-Play and are not detected or installed automatically. Admin should be able to install these printers using the Add Printers.

4.1.2 More Types of Clients

Clients can access a printer immediately after an administrator adds the printer to a print server. Various types of clients should be able to connect to the print server including the following:

- **Windows 2000, Windows NT, and Windows 95/98 clients** require no additional configuration after the administrator has installed.
- **Windows 3.*x*, Windows for Workgroups, and MS-DOS clients** require 16-bit printer drivers on each client.
- **NetWare clients** require File and Print Services for NetWare installed on the print server and IPX/SPX-compatible transport on the print server and on each client.
- **Macintosh clients** require Print Services for Macintosh installed on the print server and the Appletalk transport on the print server and on each client.
- **UNIX clients** require Print Services for UNIX installed on the print server. UNIX clients that support the line printer remote (LPR) specification connect to a print server using the Line Printer Daemon (LPD) service.
- **Any client that supports Internet Printing Protocol (IPP) 1.0** can print to a print server using HTTP.

4.1.3 Advanced Printing Features

Users can now choose advanced printing features on most printers to perform the following tasks:

- **Print multiple pages on one page.** This feature saves paper by shrinking several pages and printing them on the same page.
- **Print multiple copies.** This capability is supported even for printers that can ordinarily handle only one copy.
- **Print pages in the correct order.** Some printers print pages in reverse order.

4.1.4 Simplified Print Configuration and User Interface

For the administrator, The Print Server should provide setup tools for common network configurations (including the new Standard TCP/IP Port for TCP/IP printers connected directly to the network—see next subsection). The printer interface should make it easier for both administrators and end-users to configure and manage their printing needs. The new interface includes:

- Common dialog box combining printer properties and document printing.

- Simplified Add Printer wizard.
- Simplified device settings.
- Per user printer preferences.
- Web views of the Printers folder and of the queues for each printer.

4.1.5 Standard TCP/IP Port Monitor

The new standard port monitor connects a print server to network interface printers that use the TCP/IP protocol. It replaces the LPRMON protocol for TCP/IP printers connected directly to the network through a network adapter. A standard port simplifies installation of most TCP/IP printers by automatically detecting the network settings needed to print.

4.1.6 Remote Port Administration

Admin should be able to remotely manage and configure printers from any Print Server. This feature should be supported for local, Standard TCP/IP, and LPRMON ports.

4.1.7 Easy-to-Find Network Printers Using Directory Services

In a domain environment, the easiest way to manage, locate, and connect to printers is through Directory Services. It should be by default, when you add a printer using the Add Printer tool and elect to share the printer, print server should publish it in the domain as an object in the Directory. Publishing (listing) printers in the Directory enables Directory clients—computers locate the most convenient printer. When a printer is removed from the server, it is unpublished by the server.

Group policies should be able to control printer defaults with respect to publishing printers are **Automatically publish new printers in the Directory** and **Allow printers to be published**. The **Allow printers to be published** group policy controls whether or not printers on that machine can be published.

Administrators should be able to publish printers on other print servers in the Directory. The group policy should **Prune printers that are not automatically republished** determine how the pruning service (automatic removal of printers) handles printers on other print servers when a printer is not available.

Users should be able to search for a printer that has been published in the Directory by feature (such as color printer), by physical location (such as the third floor in Building A), or by a combination (all color printers in Building A). A list of printers matching the given criteria is presented. Users should be able to select a listed printer and view its properties, open the print queue, or create a connection to use that printer. Users should be able to save search results for future use. Administrators should be able to create custom searches for different groups of users, and then save the result files wherever they wish—for example, on users' desktops.

4.1.8 Print Queue Monitoring

The System Monitor tool should include Print Queue object lets administrators monitor the performance of a local or remote printer. Counters should be set up for a variety of performance criteria, such as bytes printed

per second, job errors, or total pages printed.

4.1.9 User Permissions and Group Policies

After you have a printer and share it over the network, you must verify that users have the appropriate permissions. Printer permissions control not only who can print, but also which printing tasks a user can perform. The three levels of printer permissions are:

- **Print.** By default, all users should have the Print permission as members of the Everyone group and can therefore print documents, pause, resume, start, and cancel their own documents, and can connect to a printer.
- **Manage Documents.** This permission adds the ability to control job settings for all documents as well as pause, restart, and delete all documents.
- **Manage Printer.** This permission adds a printer, changes printer properties, deletes printers, and changes printer permissions.

You should be able to set a group policy to change the default behavior of the printing environment and to provide computers and users a standard set of preferences. For example, you can restrict some groups of users from adding or deleting printers or prevent a group from using Internet printing.

4.1.10 User Settings

The ability to change personal document defaults. Users should be able to modify global personal document settings.

4.1.11 Print Server Clustering

Clustering provides transparent failover of the print server to offer the highest level of availability. For example, if you take down one print server for maintenance, users' print jobs are sent to the surviving node (print server) in the cluster. Print server should use new port monitors that automatically copy the ports and settings to both nodes.

4.1.12 Color Output Quality

Image Color Management (ICM) 2.0 technology, in conjunction with better halftone and image processing technologies, lets users reproduce documents on a printer faster, easier, and with greater color accuracy and consistency.

ICM 2.0 features include the following:

- Better color mappings between devices with various mapping conditions, such as paper type, inks, or resolutions. Print server should automatically install the printer-specific color profile at the time the printer is installed. This color profile is compliant with International Color Consortium (ICC) color standards.

- Standard color space for images exchanged between applications and the operating system.

4.1.13 Internet Printing

Print Server printing architecture should be seamlessly integrated with the Internet:

- **URL format for printer name.** You should be able to install printers though the internet. When installing a printer from the Internet, the printer's Uniform Resource Locator (URL) is the name of the printer. Administrators should be able to choose to use the URL format within an intranet. Print server should be able to process print jobs that contain URLs, it must be running Web server.
- **Web print server security.** Print server security is provided by web server. To support all browsers and all Internet clients, you should be able to choose basic authentication. *Basic authentication* (also called *clear-text authentication*) encodes the user name and password data transmissions, but can be decoded by anyone with a freely available decoding utility. Alternatively, for more restricted security, you should be able to specify one of the following:
  - **Microsoft challenge/response authentication**, which encrypts communication between a host (server) and client and is supported by Internet Explorer.
  - **Kerberos authentication**, which is the basis for both internal and intranet logon and is also supported by Internet Explorer.
  - **Digest authentication**, which sends the user name and password information over the network as a hash value. A hash message authentication code is an IP security function that verifies that the information received is identical to the information that was sent.
  - **Secure Sockets Layer (SSL) 3 authentication**, which was developed by Netscape for transmitting private documents over the Internet.
- **Web point-and-print.** Users should be able to connect to printers on the network using Web point-and-print for single-click installation of a printer.
- **Use a URL to print.** Users should be able to print over the Internet or an intranet from a desktop client to a print server using a URL. For example, a mail-order company can send its new catalog directly to the publisher's printer, provided they have permission from the publisher and the URL of the publisher's printer.
- **View or connect to printer from browser.** Administrators or users should be able to view and manage printers from any browser. They can pause, resume, or delete a print job and can view the printer and print job's status from any browser. In addition, if they use Internet Explorer (IE) version 4.0 or higher, they can connect to a printer using a browser.

5 Messaging and Collaboration Services

5.1 Mail Server Services Recommendation:

5.1.1 Web integration:

5.1.2 Multiple Message Database:

5.1.3 Fault tolerant SMTP Message Routing:

5.1.4 Administration:

5.1.5 System Monitoring:

By using a system monitoring tool you can obtain data that you can use to diagnose system problems, plan growth, and troubleshoot problems.

5.1.6 Message Security:

It allows sending and receiving secure e-mail messages over the Internet. Using SMIME standard enables the sending and receiving of signed or sealed (encrypted) Internet mail.

5.2 Client Access service recommendation

5.2.1 Web Access:

5.2.2 Unified Messaging Platform:

To deliver effective business solutions, organizations need a unified platform that enables all type of interaction using different type of messaging like sms, email, instant messaging. (e.g., SMS to email service)

5.2.3 Real time Collaboration:

Real-time collaboration services provide the immediacy of the telephone, with the features of e-mail. Instant messaging, Chat services, Data Conferencing, Audio, and video Conferencing are other features for the real time collaboration.